Escalating Cyberwar: Warlord Technology

Understanding asymmetric systems.

> *You have been found guilty.*
> *No trial was necessary, your device has testified against you.*

When one navigates corporate controlled cyberspace, the message couldn't be more clear. Governments and tech giants negotiate the terms of total and utter digital feudalism while the people are herded into systems that are explicitly designed to control them. Even while it's still possible, opting-out comes at a non-trivial cost. It is a cost that must be paid in one form or another, because refusing to do so has a grave price as well.

Understanding Warlord Technology

It's generally the case that powerful tools can be used for good or evil, but there are exceptions. Often things can be specialized for particular purposes, and those purposes

can themselves be evil ends. On it's face, facial recognition may seem like something that isn't inherently bad, but things change a great deal when it's combined with an orchestra of social manipulation and control systems. Just as a bank account is useful to have, it's a whole other can of worms once people start being de-banked for political purposes.

As such, there are many tools that would be entirely useless to a single person on their own, but are immensely useful for those who have large groups of people to manipulate. What makes these tools *asymmetric* is that the advantages are only for the wielder, and disadvantages are imposed on the subjects. Centralized social media platforms are well-suited for this. Not only are these platforms surveilling and manipulating their users, they have the capacity to lock down content only to fellow captives. This means that a public figure limiting their voice to these platforms is only able to get their voice out if they're allowed to. *Those of us who want to reach the public, and the* ***public themselves*** must do more to support independent platforms and protocols, or else we'll all remain beholden to top-down information control systems.

There is a well-earned reluctance from the public to adopt smart appliances, and other intrusive technology. When

every device is monitored and controlled by corporations in the cloud, any feature of that device being abused arbitrarily becomes an inevitability. Understanding this means that **warlord technology** is any device or system that enables someone else to have power over one or many other people. What effectively makes this technology so dangerous is the fact that it's simple to disguise the actual purpose. Tech giants offering free services in exchange for data-harvesting has successfully put many of the serious risks *out of sight and out of mind*. As governments across the world become more repressive, these risks come into view well after they could be prevented. The opposite exists as well too, it's possible for *emancipatory* technology to be developed that's useful to people generally, but fundamentally useless for anyone seeking power over others.

The *Free and Open Web* is an excellent example, independent and non-commercial websites managed by individuals using open protocols would have been a nightmare to properly index and seize control of. Because of this, people were nudged onto controlled platforms instead of self-publishing. Another example of asymmetric technology which benefits the people would be encryption and privacy tools. Those in power will always have the means and coordination to conceal their activities. Providing simple ways for users to protect their private

information increases the costs of violating people's rights exponentially, which is why these tools are often targeted by governments with any excuse they can find.

Of course, there is symmetric technology as well. Many general-purpose tools can be used for both great evil and good as well. I would argue truly asymmetric technologies are rare, or at least highly specialized. Almost everything has all kinds of potential uses that themselves can be used for benevolent or malicious choices, ultimately it's downstream of the human condition. It is important to keep in mind however, that even the most symmetric of technology can be used by those with malevolent (or indifferent) intent for malicious ends. Just as a hammer can be used to build or for cruelty, what may seem like a reasonable exchange may end up being a terrible situation.

Cyberwar on Civilians

As noted in A non-Combattant's Guide to Cyberwar, governments are increasingly treating your devices, connections, and even your mind as a national security target. Under the pretext of combating foreign funded misinformation, governments across the globe are working to secure total information dominance over their

populations. It should go without saying that this itself is inherently anti-democratic, despite being done in the name of *protecting our democracy*. Surveillance and censorship are serious problems, but very often the lede being buried is that it's just as much about *manipulation*.

A Non-Combattant's Guide to Cyberwar

Making sense of the chaos and the crossfire.

Censorship and surveillance themselves are serious attacks on the rights and liberty on civilians, outright manipulation of the public is an even graver overreach with even more troubling implications. We can not take for granted the mistake it would be to allow these measures to continue unopposed. Too many ignore the active role governments have taken in waging cyberwar on the public. While it's intuitive to many that corporations have a profit-incentive to acquire and control as much data as possible, to others it's inconceivable to many more that governments would violate their own laws to secure domestic or foreign policy objectives.

Despite the first amendment in the united states being quite clear:

> ***Congress shall make no law respecting*** *an establishment of religion, or prohibiting the free exercise thereof;* ***or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.***

The United States has an entire information control complex that involved government departments explicitly working with corporations to manipulate public discourse during the Covid Crisis. Even when the courts attempt to restrict such overreach the largely compliant media will continue the campaign of normalizing censorship and information control, essentially advocating for the nullification of the people's rights.

The Silent Invasion

The Speculative Foundation of Surveillance Behind the Ongoing Privacy Erosion

All-encompassing surveillance is bad enough, using that information to manipulate and control the public is even worse, but far more terrible is to undermine people's security. Governments across the world have made it explicitly clear that while you may nominally have the right to privacy and security, it disappears the moment it conflicts with policy objectives. Due to the power gained from limitless surveillance, you being a law-abiding citizen in good social standing means little. Free citizens across the world must find ways to reassert control and ownership over their governments, lest we all become subjects of tyrannical systems.

Digital Blockades

The greatest mistake is to always presume internet blackouts are an all-or-nothing affair. The tragic truth is that the tools of suppression can be *incredibly precise*. The public at large has been almost wholly ignorant of this, and this has enabled behavior that leaves them vulnerable. Many people are expecting a full-on "lights-out" internet blackout. In almost every case this is unnecessary, as people themselves are all too willing to

use top-down controlled platforms, self-censor and ignore practical privacy risks. The biggest challenge is that something as simple as not encrypting your DNS queries by using the default, allows governments to lean on service providers to seize control.

Tools of the Technocracy: #9 Internet Shutdowns

Information control is the root of modern tyranny.

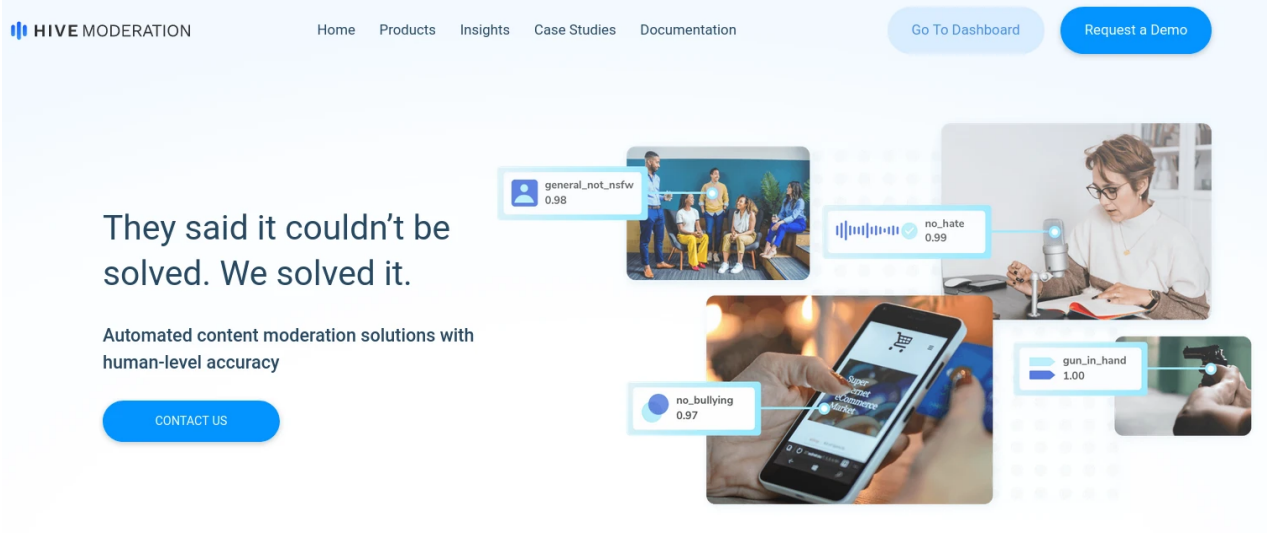
It is almost cliche these days, that governments will do everything in their power to suppress genuinely useful information in a crisis when it plays to their advantage. It's important not to be naive about corporations as well. They are every bit as capable of egregious abuses. Public-Private partnerships have worked to transform our *turn-key totalitarianism* into an unending ratchet of tyranny. As economic, social, and political power concentrates, it can be harder and harder for truly independent infrastructure to operate in a neutral way, if not outright impossible. Over time, it can be too odious for even willing infrastructure providers to withstand the pressure to

participate in censorship. No dissident or marginalized person can actually rely on a business or institution putting their needs ahead of the it's existence. This means that as more people conform to information control, and are compliant with ever more restrictive technology, the harder it is for people at all levels of society to break free. This is especially true for those who are disadvantaged.

Ultimately the more capable our devices are the more leverage they can potentially have over the public. We must be vigilant to not enable governments, corporations, or other malevolent entities to leverage them against us. Legislative restrictions are not sufficient to prevent abuse. Citizens must be well-educated on the risks, where possible devices & systems must be properly verifiable and secure, lastly there must be severe consequences for abuse. In the name of fighting terrorism or other threats the French government is introducing powers to leverage every device a person has against them. Even if one agrees that this power is warranted in this specific circumstance, there is no guarantee that such powers won't be generalized over time. In fact, even very specific measures preventing such abuse have consistently been ignored by all kinds of governments under all kinds of pretexts.

Full-Auto Tyranny

We already live in a world where the state of cyberspace has profound impacts on how people behave outside of it. As it currently exists, the majority of cyberspace is dominated by Corporations, Governments, and other un-accountable entities. The dream of an “information super-highway” where people of all backgrounds can meaningfully create, learn and share together is in dire peril.



Hive Moderation is a real-time AI censorship tool.

“Moderation at scale” effectively means mass information control. Instead of merely ranching people onto platforms to serve them targeted ads, now the capabilities exist to immediately prevent inconvenient discourse, or even entirely shape discussion. Even if people are starting to wake up to 2010s era social media, hardly anyone is

prepared for the impacts created by upcoming and state-of-the art systems of control. It is critical to not let the inefficiencies and short-comings of existing systems lure you into a false sense of security when it comes to future threats.

Naturally, these excesses will be demanded on the terms of safety, and preventing crime. While there are real and severe dangers in cyberspace, it is important to note that this level of control over the people is entirely unprecedented. As these systems roll out, people will only barely have solace in their own mind, but hardly anywhere else.

Fertile ground for resistance

First and foremost, we need to strengthen our commitment to each other's inalienable human rights before nit-picking on particular technological choices.

These implications have a very real impact on our daily lives. More and more events and services are going entirely *cashless* which often requires people to use products and services with terrible privacy protections. You may have been able to opt-out of these systems yourself, but what can be done to protect others from

them? What about people who are perfectly fine with trading a total online-enabled surveillance grid if it makes their life easier? What about those who genuinely lack the time and energy to devote to opting out? Even entire cities can fold to the pressure of conforming to these trends in the face of powerful incentives.

Regardless of one's chosen level of participation, it is absolutely vital that we get others to understand the risks. With that understanding it can be much easier to individually and collectively negotiate vital protections that need to be available, and encourage investment in new products and techniques. For now, it seems that the demand for tools and systems that don't impact one's privacy and freedom is far too low. We are all responsible for if not outright raising that demand, and communicating it effectively.

It's a shame that the benefits of free and open dialogue are only readily apparent when they're gone. The capability for people across the world to freely exchange information near instantaneously is absolutely critical to people's life and liberty. It is vital that humanity maintains this critical component in holding the powerful accountable. Allowing the massive power structures that exist to have a veto power over people's communication is too large an advantage to passively permit.

In times of inflamed tensions, social unrest, or even economic troubles, it can be very tempting for governments to *smooth things over* by constraining people's ability to learn, create and share with each other. In many cases this undermines the peoples own ability to adapt to changes, potentially being caught unaware of dangers the state failed to (or chose not to) communicate. These days, whenever a nation adopts a particularly egregious control measure, regardless of pretext or circumstances other nations aren't far behind. While the assaults on people's privacy and digital autonomy are top-down they are enabled or even welcomed by particular behaviors that we have a responsibility to stop, and prevent.

The major challenge is that people from all walks of life nee
the ave
to eir
blu

Gabriel

Published: Jul 17 2023

Tags: Technocracy Decentralization Information Control Operation: Bankroll Operation: Shadow Operation: Hearth Cyberwar

The Coordinated Attack on Cyberspace

The technocracy is grabbing new powers to control your digital life

In defense of anonymity

Don't let the trolls bait you into turning on privacy